

Министерство цифрового развития, связи и
массовых коммуникаций Российской Федерации

Федеральное государственное бюджетное образовательное учреждение высшего
образования «Сибирский государственный университет телекоммуникаций и
информатики» (СибГУТИ)

Кафедра вычислительных систем

ОТЧЕТ
по расчёто-графическому заданию
по дисциплине «**Сети ЭВМ и телекоммуникации**»

Выполнил:
студент гр. ИС-242
«__» мая 2024 г.

_____ / .B. . /

Проверил:
«__» июня 2024 г. _____ /Мамойленко.С.Н/

Оценка « _____ »

Новосибирск 2024 г.

ОГЛАВЛЕНИЕ

ПОСТАНОВКА ЗАДАЧИ

3

ВЫПОЛНЕНИЕ РАБОТЫ

5

ПОСТАНОВКА ЗАДАЧИ

1. Соберите конфигурацию сети, представленной на рисунке 1. Коммутаторы на рисунке – это виртуальные коммутаторы VirtualBox, работающие в режиме Host-only network, доступ в сеть интернет сконфигурирован для маршрутизаторов mt-01 и mt-03 через сеть NAT в VirtualBox. Во всех сетевых устройствах (кроме hostмашины) интерфейс ether4 должен быть использован как management интерфейс (схема подключения – NAT), остальные интерфейсы используются для передачи данных (далее они будут называться «рабочими»).

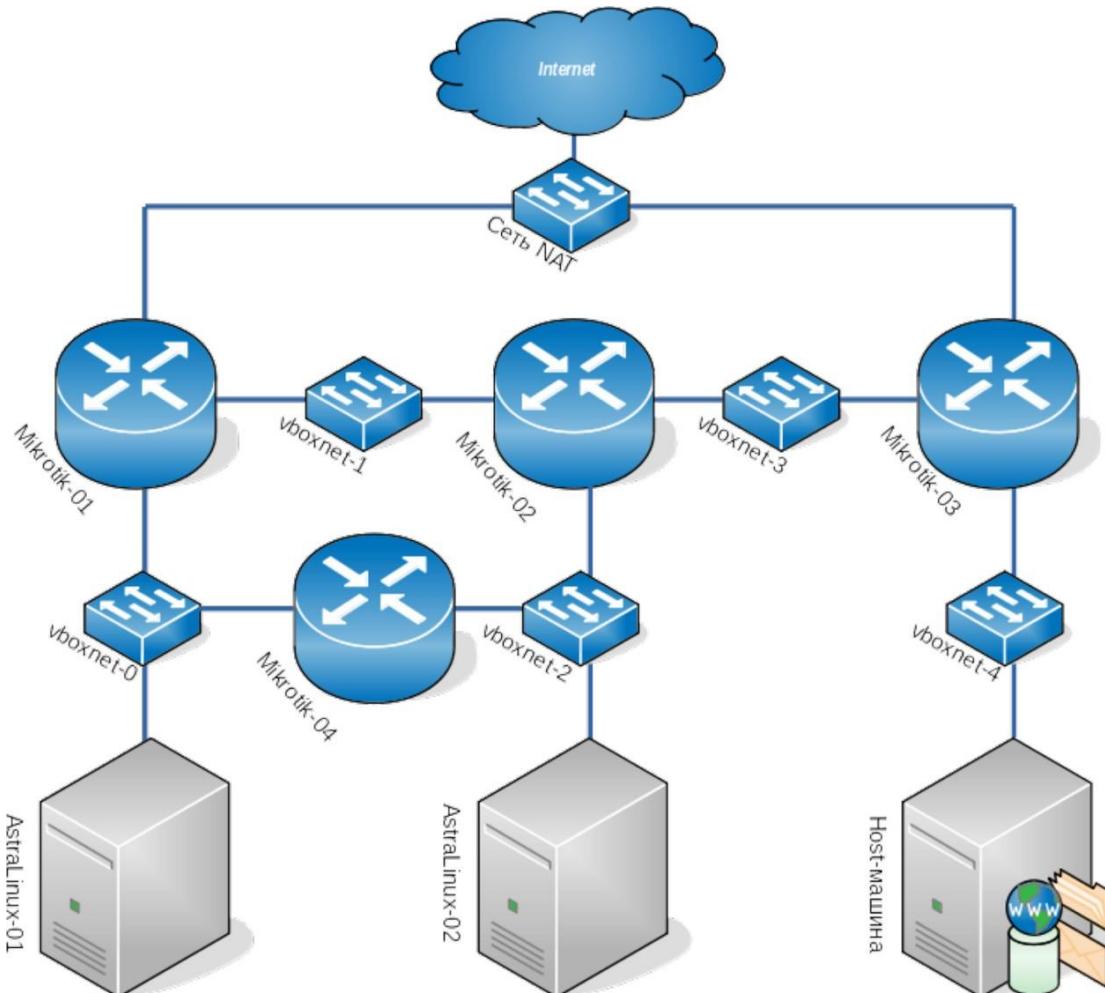


Рисунок 1 — Схема сети для расчетно-графического задания

2. Задайте уникальные сетевые имена всем сетевым устройствам (допускается хост машине не назначать сетевое имя). На management интерфейсах настройте проброс портов (DNAT) с локального интерфейса host-машины до web интерфейса маршрутизатора и до ssh на виртуальных машинах AstraLinux (доступ по ssh должен осуществляться по открытому ключу).
3. Объедините все рабочие порты коммутаторов в сетевые мосты. Настройте работу протокола STP. Покажите в каком состоянии оказались порты маршрутизаторов и объясните почему. Измените настройки протокола STP так, чтобы корневым коммутатором был mt-02, а mt-04 был резервным.
4. Вам выделен диапазон IPv4 адресов 10.10.N.0/24, где N – это Ваш порядковый номер в журнале преподавателя. Разделите полученный диапазон на максимально возможное количество подсетей так, чтобы каждая подсеть могла адресовать до 6 узлов. Выберите

один из полученных диапазонов и сконфигурируйте соответствующим образом интерфейсы виртуальных машин и сетевых мостов на маршрутизаторах. Убедитесь, что есть связь между всеми указанными сетевыми устройствами. Для доказательства наличия связи используйте захват пакетов с помощью Wireshark.

5. На маршрутизаторах mt-01, mt-02, mt-03 создайте VLAN с номером 2, которая будет использоваться для доступа в сеть NAT. Настройте VirtualBox так, чтобы в сети NAT функционировал DHCP, и он раздавал IPv4 адреса из другого диапазона, чем выбран в пункте 4. На каждом из этих маршрутизаторов настройте dhcp-client так, чтобы автоматически конфигурировались соответствующие интерфейсы и все эти маршрутизаторы получили доступ в сеть Интернет (интерфейс маршрутизатора mt-02 в сети vboxnet2 пока в эту VLAN не включается). Определите какие адреса назначены на маршрутизаторах.
6. На всех маршрутизаторах создайте VLAN с номером 3, которая будет использоваться для доступа в сеть vboxnet4. Для адресации узлов в этой сети используется ещё один диапазон IPv4 адресов, полученных в п.4. Назначьте адреса всем сетевым устройствам сети (маршрутизаторам, виртуальным машинам, хост-машине). Какие интерфейсы пингуются между собой? Примечание: на виртуальных машинах должны быть созданы виртуальные интерфейсы для доступа в тегированную VLAN с номером 3.
7. На маршрутизаторе mt-01 настройте правило трансляции адресов таким образом, чтобы предоставить виртуальной машине astra1 доступ в интернет из нетегируемой сети. Измените конфигурацию mt-02 таким образом, чтобы обеспечить доступ к тегированной VLAN с номером 2 через интерфейс в сети vboxnet2. На виртуальной машине astra2 настройте виртуальный интерфейс таким образом, чтобы он получил настройки из сети NAT и получил доступ в сеть Интернет.
8. На всех маршрутизаторах настройте протокол динамической маршрутизации RIP
9. Вам выделен диапазон IPv6 адресов FD00:::/64, где YEAR – год Вашего рождения, MONTH – месяц Вашего рождения. На маршрутизаторе mt-03 создайте DHCP-сервер для распределения префиксов IPv6 из выделенного Вам диапазона.
10. На маршрутизаторе mt-03 из созданного пула адресов настройте IPv6 адрес на интерфейс в VLAN с номером 3 с трансляцией префикса. Убедитесь, что хост машина была сконфигурирована с адресом из транслируемого диапазона.
11. На маршрутизаторе mt-01 настройте DHCP клиента так, чтобы он получил префикс для распределения. Из полученного пула IPv6 адресов назначьте адрес на интерфейс сетевого моста и настройте распространение префикса. На виртуальных машинах astralinux настройте автоматическую конфигурацию IPv6 адресов.
12. Настройте маршрутизацию для IPv6 таким образом, чтобы пинговались виртуальные машина и host-машина.
13. На виртуальной машине astra2 проверьте настройки DNS клиента. Убедитесь, что запросы по умолчанию передаются на DNS с адресом 8.8.8.8.
14. Используя консольные утилиты с узла astra2 найдите всю возможную информацию о DNS-зоне csc.sibsutis.ru, IPv4 имени ans.csc.sibsutis.ru, IPv4 адрес домена mail.ru и обо всех IP адресах, найденных для домена mail.ru.

ВЫПОЛНЕНИЕ РАБОТЫ

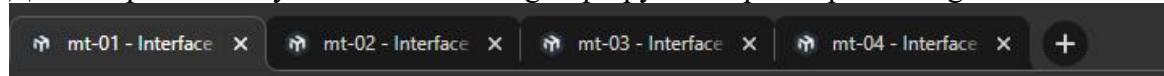
При выполнении работы было сделано следующее:

- Собрана конфигурация в соответствии с заданием.
- Всем сетевым устройствам кроме хост-машины заданы уникальные сетевые имена, настроен проброс портов до веб-интерфейса маршрутизаторов через NAT-интерфейс (порт роутеров - 80, порты хоста - 30001, 30002, 30003...), до ssh на виртуальных машинах astralinux (порт astralinux машин - 22, порты хоста - 30022, 30023).

Пример проброса портов на маршрутизаторе mt-01:

Правила проброса портов					
Имя	Протокол	Адрес хоста	Порт хоста	Адрес гостя	Порт гостя
Rule 1	TCP	127.0.0.1	30001		80

Демонстрация доступа ко всем WebFig маршрутизаторов через management-interface:



- Все рабочие порты коммутаторов были объединены в сетевые мосты, включён протокол STP. Демонстрация примера сетевого моста на маршрутизаторе mt-01:

1 item		#	Interface	Bridge
		0	ether1	bridge1
-	D	1	ether2	bridge1
-	D	2	ether3	bridge1

Protocol Mode none STP RSTP MSTP

Порты оказались в следующих состояниях и ролях (номер порта соответствует номеру интерфейса Ethernet-интерфейса: ether1 => Port Number = 1):

mt-01

Port Number	1	Port Number	2	Port Number	3
Role	designated port	Role	designated port	Role	root port

mt-02

Port Number	1	Port Number	2	Port Number	3
Role	alternate port	Role	designated port	Role	root port

mt-03

Port Number	1	Port Number	2	Port Number	3
Role	designated port	Role	designated port	Role	designated port

mt-04

Port Number	1	Port Number	2
Role	root port	Role	alternate port

Состояния сетевых мостов на маршрутизаторах:

mt-01	mt-02
Root Bridge <input type="checkbox"/>	Root Bridge <input type="checkbox"/>
Root Bridge ID 8000.08:00:27:0D:BC:34	Root Bridge ID 8000.08:00:27:0D:BC:34
Regional Root Bridge ID 0.00:00:00:00:00:00	Regional Root Bridge ID 0.00:00:00:00:00:00
Root Path Cost 10	Root Path Cost 10
Root Port ether3	Root Port ether3
mt-03	mt-04
Root Bridge <input checked="" type="checkbox"/>	Root Bridge <input type="checkbox"/>
Root Bridge ID 8000.08:00:27:0D:BC:34	Root Bridge ID 8000.08:00:27:0D:BC:34
Regional Root Bridge ID 0.00:00:00:00:00:00	Regional Root Bridge ID 0.00:00:00:00:00:00
Root Path Cost 0	Root Path Cost 20
Root Port none	Root Port ether1

Изменим настройки протокола STP так, чтобы корневым коммутатором был mt-02, а mt-04 был резервным: уменьшим приоритет bridge1 в поле Priority на mt-02 до 7000 (стандартный - 8000), а на mt-04 - до 7500. Теперь bridge1 на mt-02 является корневым, а bridge1 на mt-04 станет таковым, если корневой выйдет из строя или отключится.

mt-02	mt-04
Protocol Mode <input type="radio"/> none <input type="radio"/> STP <input checked="" type="radio"/> RSTP <input type="radio"/> MSTP	Protocol Mode <input type="radio"/> none <input type="radio"/> STP <input checked="" type="radio"/> RSTP <input type="radio"/> MSTP
Priority 7000 hex	Priority 7500 hex
Root Bridge <input checked="" type="checkbox"/>	Root Bridge <input type="checkbox"/>
Root Bridge ID 7000.08:00:27:EF:2D:83	Root Bridge ID 7000.08:00:27:EF:2D:83
Regional Root Bridge ID 0.00:00:00:00:00:00	Regional Root Bridge ID 0.00:00:00:00:00:00
Root Path Cost 0	Root Path Cost 10
Root Port none	Root Port ether2
Port Count 3	Port Count 2
Designated Port Count 3	Designated Port Count 1
MST Config Digest	MST Config Digest

4. Выделенный диапазон 10.10.3.0/24 разделим на максимально возможное количество подсетей так, чтобы каждая подсеть могла адресовать до 6 узлов. Для этого необходимо выделить последние 3 бита четвёртого октета адреса IPv4, маска подсети соответственно

будет составлять 29 битов. Однако чтобы не столкнуться с проблемами при выделении 7 IP-адресов в сети (чтобы не давать какому-то устройству адрес самой сети), назначим маску /28, в которой будет свободно адресовать 14 хостов.

Subnet address	Netmask	Range of addresses	Useable IPs	Hosts
10.10.3.0/28	255.255.255.240	10.10.3.0 - 10.10.3.15	10.10.3.1 - 10.10.3.14	14
10.10.3.16/28	255.255.255.240	10.10.3.16 - 10.10.3.31	10.10.3.17 - 10.10.3.30	14
10.10.3.32/28	255.255.255.240	10.10.3.32 - 10.10.3.47	10.10.3.33 - 10.10.3.46	14
10.10.3.48/28	255.255.255.240	10.10.3.48 - 10.10.3.63	10.10.3.49 - 10.10.3.62	14
10.10.3.64/28	255.255.255.240	10.10.3.64 - 10.10.3.79	10.10.3.65 - 10.10.3.78	14
10.10.3.80/28	255.255.255.240	10.10.3.80 - 10.10.3.95	10.10.3.81 - 10.10.3.94	14
10.10.3.96/28	255.255.255.240	10.10.3.96 - 10.10.3.111	10.10.3.97 - 10.10.3.110	14
10.10.3.112/28	255.255.255.240	10.10.3.112 - 10.10.3.127	10.10.3.113 - 10.10.3.126	14
10.10.3.128/28	255.255.255.240	10.10.3.128 - 10.10.3.143	10.10.3.129 - 10.10.3.142	14
10.10.3.144/28	255.255.255.240	10.10.3.144 - 10.10.3.159	10.10.3.145 - 10.10.3.158	14
10.10.3.160/28	255.255.255.240	10.10.3.160 - 10.10.3.175	10.10.3.161 - 10.10.3.174	14
10.10.3.176/28	255.255.255.240	10.10.3.176 - 10.10.3.191	10.10.3.177 - 10.10.3.190	14
10.10.3.192/28	255.255.255.240	10.10.3.192 - 10.10.3.207	10.10.3.193 - 10.10.3.206	14
10.10.3.208/28	255.255.255.240	10.10.3.208 - 10.10.3.223	10.10.3.209 - 10.10.3.222	14
10.10.3.224/28	255.255.255.240	10.10.3.224 - 10.10.3.239	10.10.3.225 - 10.10.3.238	14
10.10.3.240/28	255.255.255.240	10.10.3.240 - 10.10.3.255	10.10.3.241 - 10.10.3.254	14

Полученные подсети можно увидеть на таблице левее.

Выберем первый из полученных диапазонов (10.10.3.1-10.10.3.14). На маршрутизаторах меню IP -> Addresses назначим нужные адреса на нужные сетевые мосты, на машинах astralinux зададим статические IP-адреса в файле /etc/network/interfaces.d/eth0.

mt-01
mt-02



mt-03

✚ 10.10.3.3/28 10.10.3.0 bridge1

mt-04

✚ 10.10.3.4/28 10.10.3.0 bridge1

astral1

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP>
      link/ether 08:00:27:f6:f0:c2 brd
      inet 10.10.3.5/28 brd 10.10.3.15
```

astra2

```
eth0: <BROADCAST,MULTICAST,UP,LOWER_UP>
      link/ether 08:00:27:40:31:47 brd ff:ff:ff:ff:ff:ff
      inet 10.10.3.6/28 brd 10.10.3.15 scope
```

Убедимся, что между всеми указанными сетевыми устройствами есть связь: проведём ping между всеми узлами и покажем некоторые такие попытки для наглядности.

mt-03 -> все устройства

```
[admin@mt-03] > ping 10.10.3.1
SEQ HOST SIZE TTL TIME STATUS
  0 10.10.3.1          56  64 371us
  1 10.10.3.1          56  64 392us
  sent=2 received=2 packet-loss=0% min-rtt=371us avg-rtt=381us
  max-rtt=392us

[admin@mt-03] > ping 10.10.3.2
SEQ HOST SIZE TTL TIME STATUS
  0 10.10.3.2          56  64 479us
  1 10.10.3.2          56  64 284us
  sent=2 received=2 packet-loss=0% min-rtt=284us avg-rtt=381us
  max-rtt=479us

[admin@mt-03] > ping 10.10.3.4
SEQ HOST SIZE TTL TIME STATUS
  0 10.10.3.4          56  64 701us
  1 10.10.3.4          56  64 428us
  sent=2 received=2 packet-loss=0% min-rtt=428us avg-rtt=564us
  max-rtt=701us
```

```
[admin@nt-031 ~] > ping 10.10.3.5
SEQ HOST SIZE TTL TIME STATUS
 0 10.10.3.5 56 64 1ms252us
 1 10.10.3.5 56 64 600us
sent=2 received=2 packet-loss=0% min-rtt=600us avg-rtt=926us
max-rtt=1ms252us

[admin@nt-031 ~] > ping 10.10.3.6
SEQ HOST SIZE TTL TIME STATUS
 0 10.10.3.6 56 64 425us
 1 10.10.3.6 56 64 371us
sent=2 received=2 packet-loss=0% min-rtt=371us avg-rtt=398us
max-rtt=425us
```

astra2 -> все устройства

```
root@astra2:~# ping 10.10.3.1
PING 10.10.3.1 (10.10.3.1) 56(84) bytes of data.
64 bytes from 10.10.3.1: icmp_seq=1 ttl=64 time=0.365 ms
^C
--- 10.10.3.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.365/0.365/0.365/0.000 ms
root@astra2:~# ping 10.10.3.2
PING 10.10.3.2 (10.10.3.2) 56(84) bytes of data.
64 bytes from 10.10.3.2: icmp_seq=1 ttl=64 time=0.227 ms
^C
--- 10.10.3.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.227/0.227/0.227/0.000 ms
root@astra2:~# ping 10.10.3.3
PING 10.10.3.3 (10.10.3.3) 56(84) bytes of data.
64 bytes from 10.10.3.3: icmp_seq=1 ttl=64 time=0.371 ms
^C
--- 10.10.3.3 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.371/0.371/0.371/0.000 ms
root@astra2:~# ping 10.10.3.4
PING 10.10.3.4 (10.10.3.4) 56(84) bytes of data.
64 bytes from 10.10.3.4: icmp_seq=1 ttl=64 time=0.235 ms
^C
--- 10.10.3.4 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.235/0.235/0.235/0.000 ms
root@astra2:~# ping 10.10.3.5
PING 10.10.3.5 (10.10.3.5) 56(84) bytes of data.
64 bytes from 10.10.3.5: icmp_seq=1 ttl=64 time=0.369 ms
^C
--- 10.10.3.5 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.369/0.369/0.369/0.000 ms
```

5. На маршрутизаторах mt-01, mt-02 и mt-03 создадим виртуальные интерфейсы VLAN с ID 2, которые будут использоваться для доступа в сеть NAT (внешнюю сеть Интернет).

Enabled	<input checked="" type="checkbox"/>
Name	vlan2
Type	VLAN
MTU	1500
Actual MTU	1500
L2 MTU	65531
MAC Address	08:00:27:9A:BC:DC
ARP	enabled
ARP Timeout	▼
VLAN ID	2
Interface	bridge1 ▾

Настроим сеть NAT в VirtualBox так, чтобы в ней функционировал DHCP-сервер, раздающий IPv4 адреса из второго диапазона подсетей (10.10.3.19-10.10.3.29) DHCP-клиентам на VLAN2-интерфейсах маршрутизаторов, и они получили доступ в сеть Интернет.

```
C:\Program Files\Oracle\VirtualBox>VBoxManage dhcpserver modify --network=natnet
--server-ip=10.10.3.18 --lower-ip=10.10.3.19 --upper-ip=10.10.3.29 --netmask=255.
255.255.240
```

Распределим нужные интерфейсы по VLAN-сетям.

Во-первых, зададим PVID=2 интерфейсам, соединённым с сетью NAT на mt-01 и mt-03:

(ether3 mt-01 & ether3 mt-03) **PVID**

Далее на интерфейсы, лежащие между mt-01, mt-02 и mt-03 зададим тегированный трафик, т.к. в этих каналах будут присутствовать и другие VLAN-сети.

mt-01

	Bridge	VLAN IDs	Current Tagged	Current Untagged
- D	bridge1	2	bridge1, ether2	ether3
-	D	bridge1	1	bridge1, ether1, ether2

mt-02

	Bridge	VLAN IDs	Current Tagged	Current Untagged
-	D	bridge1	1	bridge1, ether1, ether2, ether3
- D	bridge1	2	bridge1, ether1, ether3	

mt-03

	Bridge	VLAN IDs	Current Tagged	Current Untagged
-	D	bridge1	1	bridge1, ether1, ether2
- D	bridge1	2	bridge1, ether1	ether3

Определим, какие адреса теперь назначены на интерфейсах маршрутизаторов:

DHCP-клиенты:

mt-01

vlan2	yes	yes	10.10.3.19/28	vlan2	yes	yes	10.10.3.21/28
mt-03							
vlan2	yes	yes	10.10.3.20/28				

Получение IPv4-адреса по протоколу DHCP от сети NAT: (mt-02)

9086 1089.495296	0.0.0.0	255.255.255.255	DHCP	346 DHCP Discover	- Transaction ID 0x1fd8687f
9087 1089.495876	10.10.3.18	255.255.255.255	DHCP	594 DHCP Offer	- Transaction ID 0x1fd8687f
9088 1089.495961	0.0.0.0	255.255.255.255	DHCP	346 DHCP Request	- Transaction ID 0x1fd8687f
9089 1089.499181	10.10.3.18	255.255.255.255	DHCP	594 DHCP ACK	- Transaction ID 0x1fd8687f
<hr/>					
Frame 9089: 594 bytes on wire (4752 bits), 594 bytes captured (4752 bits) Ethernet II, Src: PcsCompu_e6:cb:60 (08:00:27:e6:cb:60), Dst: Broadcast (ff:ff:ff:ff:ff:ff) 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2 Internet Protocol Version 4, Src: 10.10.3.18, Dst: 255.255.255.255 User Datagram Protocol, Src Port: 67, Dst Port: 68 Dynamic Host Configuration Protocol (ACK) Message type: Boot Reply (2) Hardware type: Ethernet (0x01) Hardware address length: 6 Hops: 0 Transaction ID: 0x1fd8687f Seconds elapsed: 0 Bootp flags: 0x0000 (Unicast) Client IP address: 0.0.0.0 Your (client) IP address: 10.10.3.21					
<hr/>					
0030	06 00 1f d8 68 7f				
0040	03 15 00 00 00 00				
0050	00 00 00 00 00 00				
0060	00 00 00 00 00 00				
0070	00 00 00 00 00 00				
0080	00 00 00 00 00 00				
0090	00 00 00 00 00 00				
00a0	00 00 00 00 00 00				
00b0	00 00 00 00 00 00				
00c0	00 00 00 00 00 00				
00d0	00 00 00 00 00 00				
00e0	00 00 00 00 00 00				
00f0	00 00 00 00 00 00				
0100	00 00 00 00 00 00				
0110	00 00 00 00 00 00				
0120	0a 0a 03 12 35 01				
0130	0a 03 09 06 04 c0				

Пробуем пинговать DNS-сервер Google с одного из полученных адресов - всё работает.

```
[admin@mt-02] > ping 8.8.8.8
SEQ HOST SIZE TTL TIME STATUS
 0 8.8.8.8 56 113 82ms754us
 1 8.8.8.8 56 113 86ms633us
sent=2 received=2 packet-loss=0% min-rtt=82ms754us avg-rtt=84ms693us
max-rtt=86ms633us
```

6. На всех устройствах создадим новые виртуальные интерфейсы VLAN для доступа к VLAN с ID 3, и настроим в этой VLAN тегированный трафик для доступа в сеть vboxnet4 через созданные интерфейсы VLAN3.

Для адресации узлов в этой сети используем третий диапазон из IPv4 адресов, полученных в пункте 4 (10.10.3.33-10.10.3.46).

mt-01	Enabled <input checked="" type="checkbox"/>	Name <input type="text" value="vlan3"/>
Address <input type="text" value="10.10.3.33/28"/>	Type VLAN	
Network ▲ <input type="text" value="10.10.3.32"/>	MTU <input type="text" value="1500"/>	
Interface <input type="button" value="vlan3"/>	Actual MTU	
mt-02	Enabled <input checked="" type="checkbox"/>	MAC Address
Address <input type="text" value="10.10.3.34/28"/>	ARP <input type="button" value="enabled"/>	
Network ▲ <input type="text" value="10.10.3.32"/>	ARP Timeout	
Interface <input type="button" value="vlan3"/>	VLAN ID <input type="text" value="3"/>	
mt-03	mt-04	

Enabled	<input checked="" type="checkbox"/>
Address	10.10.3.35/28
Network	▲ 10.10.3.32
Interface	vlan3 ▼

Enabled	<input checked="" type="checkbox"/>
Address	10.10.3.36/28
Network	▲ 10.10.3.32
Interface	vlan3 ▼

```
astra1 astra2  
eth0.3@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP>  
          link/ether 08:00:27:f6:f0:c2 brd f0:ff:ff:ff:ff:ff  
          inet 10.10.3.37/28 brd 10.10.3.47  
eth0.3@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP>  
          link/ether 08:00:27:40:31:47 brd f0:ff:ff:ff:ff:ff  
          inet 10.10.3.38/28 brd 10.10.3.47
```

mt-01

	Bridge	VLAN IDs	Current Tagged	Current Untagged
- D	bridge1	2	bridge1, ether2	ether3
- D	bridge1	3	bridge1, ether1, ether2	
- D	bridge1	1		bridge1, ether1, ether2

mt-02

	Bridge	VLAN IDs	Current Tagged	Current Untagged
[D]	bridge1	3	bridge1, ether1, ether2, ether3	
[]	D	bridge1	1	bridge1, ether1, ether2, ether3
[D]		bridge1	2	bridge1, ether1, ether3

mt-03: ether2: PVID 3

mt-04

Bridge	VLAN IDs	Current Tagged	Current Untagged
bridge1	1		bridge1, ether1, ether2
bridge1	3	bridge1, ether1, ether2	

Проверим, какие интерфейсы пингуются: как и ожидалось, все пингуются между собой и в сетях vboxnet0, vboxnet3 можно увидеть тегированный трафик к машинах astralinux, а в vboxnet4 - нетегированный к хосту.

Тегированный трафик в vboxnet3:

5385	3262.440511	10.10.3.38	10.10.3.34	ICMP	102 Echo (ping) request	i
5386	3262.440697	10.10.3.34	10.10.3.38	ICMP	102 Echo (ping) reply	i
5387	3263.310696	PcsCompu_ef:0:67:2e	Spanning-tree-(for-... STP		53 RST. Root = 28672/0/0	
5388	3263.464763	10.10.3.38	10.10.3.34	ICMP	102 Echo (ping) request	i
5389	3263.464984	10.10.3.34	10.10.3.38	ICMP	102 Echo (ping) reply	i

Frame 5389: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
 Ethernet II, Src: PcsCompu_ef:2d:83 (08:00:27:ef:2d:83), Dst: PcsCompu_40:31:47 (08:00:27:40:
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 3
Internet Protocol Version 4, Src: 10.10.3.34, Dst: 10.10.3.38
Internet Control Message Protocol

Нетегированный трафик в vboxnet4:

94	73.136310	10.10.3.35	10.10.3.39	ICMP	70 Echo (ping) request
95	73.136376	10.10.3.39	10.10.3.35	ICMP	70 Echo (ping) reply
Frame 94: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF_{...}					
Ethernet II, Src: PcsCompu_0d:bc:34 (08:00:27:0d:bc:34), Dst: 0a:00:27:00:00:0e (0a:00:27:00:00:0e)					
Internet Protocol Version 4, Src: 10.10.3.35, Dst: 10.10.3.39					
Internet Control Message Protocol					

7. На маршрутизаторе mt-01 настроим правила трансляции адресов таким образом, чтобы предоставить виртуальной машине astra1 доступ в интернет из untagged сети.

Во-первых, выключим default route с management-интерфейса, чтобы при трансляции

адреса пакеты шли не на NAT-интерфейс, а в сеть NAT.

Перенастроим также default route на astra1 с management-интерфейса на eth0:

```
owner@astra1:~$ sudo ip route del default
owner@astra1:~$ sudo ip route add default via 10.10.3.1 dev eth0
```

В IP -> Firewall -> NAT Mikrotik добавим новое правило на цепочку src-nat, чтобы пакеты с адреса astra1 перенаправлялись на интерфейс wlan2, который соединён с нетегированной сетью NAT.

Action	Chain	Src. Address	Dst. Address	Src. Address List	Dst. Address List	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf..
masquerade	srcnat	10.10.3.5									vlan2

Проверяем ping с astra1 до DNS-сервера Google: всё работает!

```
root@astra1:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=112 time=83.9 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=112 time=83.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=112 time=83.4 ms
^C
--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 83.478/83.679/83.996/0.226 ms
root@astra1:~#
```

Проверяем трафик: тег отсутствует!

3955	2176.663748	10.10.3.5	8.8.8.8	ICMP	98 Echo (ping) request
3956	2176.747130	8.8.8.8	10.10.3.5	ICMP	98 Echo (ping) reply
Frame 3956: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)					
Ethernet II, Src: PcsCompu_9a:bc:dc (08:00:27:9a:bc:dc), Dst: PcsCompu_f6:f0:c2 (08:00:27:f6:...)					
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.10.3.5					
Internet Control Message Protocol					

Теперь изменим конфигурацию таким образом, чтобы обеспечить доступ astra2 к тегированной VLAN-2 через ether2 mt-02. Для этого нужно создать новый интерфейс eth0.2 на astra2 для доступа к тегированной VLAN-2 и в mt-02 поставить тегированный трафик на выходе к astra2:

```
root@astra2:~# ip link add link eth0 name eth0.2 type vlan id 2
```

		Bridge	VLAN IDs	Current Tagged	Current Untagged
- [D]		bridge1	2	bridge1, ether1, ether2, ether3	

Настроим получение IP-адреса для нового интерфейса на astra2 в файле /etc/network/interfaces.d/eth0 зададим параметры для интерфейса eth0.2:

```
auto eth0.2
iface eth0.2 inet dhcp
```

Включим интерфейс eth0.2: он получил адрес через DHCP-сервер на сети NAT и теперь имеет доступ в тегированную сеть VLAN2.

```
root@astra2:~# ifup eth0.2
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0.2/08:00:27:40:31:47
Sending on  LPF/eth0.2/08:00:27:40:31:47
Sending on  Socket/fallback
DHCPDISCOVER on eth0.2 to 255.255.255.255 port 67 interval 7
DHCPREQUEST of 10.10.3.23 on eth0.2 to 255.255.255.255 port 67
DHCPoffer of 10.10.3.23 from 10.10.3.19
DHCPACK of 10.10.3.23 from 10.10.3.19
bound to 10.10.3.23 -- renewal in 296 seconds.
```

Меняем маршрут по умолчанию на новую сеть: выключаем старый маршрут по умолчанию через management-интерфейс и перезапускаем eth0.2, чтобы получить маршрут от DHCP-сервера сети NAT. Пробуем пинговать DNS-сервер Google с нового интерфейса eth0.2: всё работает отлично.

```
root@astra2:~# sudo ip route del default
```

```

root@astra2:~# ifup eth0.2
Internet Systems Consortium DHCP Client 4.3.5
Copyright 2004-2016 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0.2/08:00:27:40:31:47
Sending on  LPF/eth0.2/08:00:27:40:31:47
Sending on  Socket/fallback
DHCPDISCOVER on eth0.2 to 255.255.255.255 port 67 interval 3
DHCPREQUEST of 10.10.3.23 on eth0.2 to 255.255.255.255 port 67
DHCPoffer of 10.10.3.23 from 10.10.3.19
DHCPACK of 10.10.3.23 from 10.10.3.19
bound to 10.10.3.23 -- renewal in 254 seconds.
root@astra2:~# route -n
Kernel IP routing table
Destination      Gateway          Genmask        Flags Metric Ref  Use Iface
0.0.0.0          10.10.3.17    0.0.0.0        UG   0      0      0 eth0.2
10.0.3.0         0.0.0.0        255.255.255.0  U     0      0      0 eth1
10.10.3.0        0.0.0.0        255.255.255.240 U     0      0      0 eth0
10.10.3.16       0.0.0.0        255.255.255.240 U     0      0      0 eth0.2
10.10.3.32       0.0.0.0        255.255.255.240 U     0      0      0 eth0.3
root@astra2:~# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=86.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=83.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=83.1 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=113 time=83.0 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 83.094/83.990/86.407/1.440 ms

```

Захваченные пакеты из тегированной сети vboxnet2 с astra2:

2598	1870.316106	10.10.3.23	8.8.8.8	ICMP	102 Echo (ping) request	
2599	1870.399101	8.8.8.8	10.10.3.23	ICMP	102 Echo (ping) reply	
<hr/>						
Frame 2599: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)						
Ethernet II, Src: RealtekU_12:35:00 (52:54:00:12:35:00), Dst: PcsCompu_40:31:47 (08:00:27:40:31:47)						
802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 2						
Internet Protocol Version 4, Src: 8.8.8.8, Dst: 10.10.3.23						
Internet Control Message Protocol						

8. На всех маршрутизаторах настроим протокол динамической маршрутизации RIP. Зайдём в WebFig всех роутеров и добавим новый RIP-instance и interface template (для всех интерфейсов устройства кроме management) в меню Routing. В шаблоне интерфейсов также необязательно указывать интерфейсы, принадлежащие сетевому мосту, потому что он их всех объединяет под одним IP-адресом.

The left screenshot shows the configuration of a RIP instance named 'rip-instance-1'. It includes fields for Enabled (checked), Name (rip-instance-1), VRF (dropdown), AFI (dropdown), Input Filter (dropdown), Output Filter (dropdown), Select Output Filter (dropdown), and Redistribution (checkboxes for connected, static, rip, ospf, bgp, dhcp, modem, vpn, fantasy, copy). The 'Redistribution' section has checkboxes for connected, static, rip, ospf, bgp, dhcp, modem, vpn, fantasy, and copy.

The right screenshot shows the configuration of a RIP interface named 'rip-interface-1' for the 'rip-instance-1'. It includes fields for Enabled (checked), Name (rip-interface-1), Instance (dropdown set to 'rip-instance-1'), and Interfaces (checkboxes for bridge1, vlan2, and vlan3).

В параметре **Redistribute** укажем **connected**, **static** и **rip** для получения информации о напрямую подключенных устройствах (маршрутах), статических записей в таблицах маршрутизации и записей, полученных другим устройством также через протокол RIP.

Проверим вкладку **Neighbors** в меню RIP mt-01: появились все соседние интерфейсы

The table displays 8 items under the 'Neighbors' tab:

	Instance	Address	Routes	Packets Total	Packets Bad	Entries Bad	Last Update
D	rip-instance-1	10.10.3.2%bridge1	3	7	0	0	00:00:14
D	rip-instance-1	10.10.3.22%vlan2	3	7	0	0	00:00:14
D	rip-instance-1	10.10.3.34%vlan3	3	7	0	0	00:00:14
D	rip-instance-1	10.10.3.3%bridge1	3	6	0	0	00:00:30
D	rip-instance-1	10.10.3.20%vlan2	3	6	0	0	00:00:30
D	rip-instance-1	10.10.3.35%vlan3	3	6	0	0	00:00:30
D	rip-instance-1	10.10.3.4%bridge1	0	2	0	0	00:00:09
D	rip-instance-1	10.10.3.36%vlan3	0	2	0	0	00:00:09

Смотрим таблицы маршрутизации на роутерах: появились абсолютно все маршруты до всех устройств в сети с выставленными метриками (расстояниями).

Пример выстроенной таблицы маршрутизации в mt-01:

27 items				
		▲ Dst. Address	Gateway	Distance
-	DAd	0.0.0.0/0	10.10.3.17	1
-	Dr	10.0.5.0/24	10.10.3.36%vlan3	120
-	Dr	10.0.5.0/24	10.10.3.4%bridge1	120
-	Dr	10.0.5.0/24	10.10.3.35%vlan3	120
-	Dr	10.0.5.0/24	10.10.3.20%vlan2	120
-	Dr	10.0.5.0/24	10.10.3.3%bridge1	120
-	Dr	10.0.5.0/24	10.10.3.34%vlan3	120
-	Dr	10.0.5.0/24	10.10.3.22%vlan2	120
-	Dr	10.0.5.0/24	10.10.3.2%bridge1	120
-	DAC	10.0.5.0/24	%ether4	
-	Dr	10.10.3.0/28	10.10.3.36%vlan3	120
-	Dr	10.10.3.0/28	10.10.3.35%vlan3	120
-	Dr	10.10.3.0/28	10.10.3.20%vlan2	120
-	Dr	10.10.3.0/28	10.10.3.34%vlan3	120
-	Dr	10.10.3.0/28	10.10.3.22%vlan2	120
-	DAC	10.10.3.0/28	%bridge1	
-	Dr	10.10.3.16/28	10.10.3.35%vlan3	120
-	Dr	10.10.3.16/28	10.10.3.3%bridge1	120
-	Dr	10.10.3.16/28	10.10.3.34%vlan3	120
-	Dr	10.10.3.16/28	10.10.3.2%bridge1	120
-	DAC	10.10.3.16/28	%vlan2	
-	Dr	10.10.3.32/28	10.10.3.4%bridge1	120
-	Dr	10.10.3.32/28	10.10.3.20%vlan2	120
-	Dr	10.10.3.32/28	10.10.3.3%bridge1	120
-	Dr	10.10.3.32/28	10.10.3.22%vlan2	120
-	Dr	10.10.3.32/28	10.10.3.2%bridge1	120
-	DAC	10.10.3.32/28	%vlan3	

9. Выделен диапазон IPv6 адресов FD00:2003:4::/64. На маршрутизаторе mt-03 создадим пул наших адресов (префикс) и DHCP-сервер для распределения префиксов IPv6 из выделенного диапазона:

Name	pool1	Enabled	<input checked="" type="checkbox"/>
Prefix	fd00:2003:4::/64	Name	dhcp-server
Prefix Length	64	Interface	bridge1
		Address Pool6	pool1
		Lease Time	3d 00:00:00

10. На маршрутизаторе mt-03 из созданного пула адресов настроим IPv6 адрес на интерфейс в VLAN3 с трансляцией префикса.

Убедимся, что хост-машина получила адрес из транслируемого диапазона: пропишем в командной строке Windows “ipconfig” и посмотрим на параметры адаптера vboxnet4:

```
Адаптер Ethernet VirtualBox Host-Only Network #5:

DNS-суффикс подключения . . . . . : 
IPv6-адрес . . . . . : fd00:2003:4:0:38df:e882:c95:6253
Временный IPv6-адрес . . . . . : fd00:2003:4:0:7c0c:1c00:d37e:f5fd
Локальный IPv6-адрес канала . . . . . : fe80::4c60:ec75:990d:fcdb%14
IPv4-адрес . . . . . : 10.10.3.39
Маска подсети . . . . . : 255.255.255.240
Основной шлюз. . . . . : fe80::a00:27ff:fe0d:bc34%14
```

11. На маршрутизаторе mt-01 настроим DHCP-клиент, чтобы он получил префикс для распределения.

Interface	Request	Pool Name	Pool Prefix Length	Use Peer DNS	Add Defa... Route	Prefix	Expires After
bridge1	prefix	dpool1	64	yes	no	fd00:2003:4:1::/64	2d 23:59:52

Из полученного пула IPv6 адресов назначим адрес на интерфейс сетевого моста и настроим распространение префикса.

Enabled	<input checked="" type="checkbox"/>
Address	fd00:2003:4:1:a00:27ff:fe9a:1
From Pool	▲ dpool1 ▼
Interface	bridge1 ▼
EUI64	<input checked="" type="checkbox"/>
Advertise	<input checked="" type="checkbox"/>

astra2

```
5: eth0.3@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1
1000
link/ether 08:00:27:40:31:47 brd ff:ff:ff:ff:ff:ff
inet 10.10.3.38/28 brd 10.10.3.47 scope global eth0
    valid_lft forever preferred_lft forever
inet6 fd00:2003:4:1:a00:27ff:fe40:3147/64 scope glo
    valid_lft 2591923sec preferred_lft 604723sec
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdi
n 1000
link/ether 08:00:27:40:31:47 brd ff:ff:ff:ff:ff:ff
inet 10.10.3.6/28 brd 10.10.3.15 scope global eth0
    valid_lft forever preferred_lft forever
inet6 fd00:2003:4:1:a00:27ff:fe40:3147/64 scope glo
    valid_lft 2591924sec preferred_lft 604724sec
```

12. Настроим маршрутизацию для IPv6

таким образом, чтобы пинговались виртуальные машины и host-машина. Для этого настроим маршрутизацию OSPF версии 3 на маршрутизаторах: добавляем все instance в

Enabled	<input checked="" type="checkbox"/>
Address	fd00:2003:4::/64
From Pool	▲ pool1 ▼
Interface	bridge1 ▼
EUI64	<input type="checkbox"/>
Advertise	<input checked="" type="checkbox"/>

Enabled	<input checked="" type="checkbox"/>
Interface	bridge1 ▼
Request	<input type="checkbox"/> info <input type="checkbox"/> address <input checked="" type="checkbox"/> prefix
Pool Name	dpool1
Pool Prefix Length	64
Prefix Hint	▲ ::/0 ▼

На виртуальных машинах astralinux автоматическую конфигурацию IPv6 адресов не требуется, так как интерфейсы сами принимают распространяемый префикс IPv6. В данном случае префикс с :0 на конце приходит от VLAN3 mt-03, :1 - от VLAN1 mt-01.

astral1

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc p
n 1000
link/ether 08:00:27:f6:f0:c2 brd ff:ff:ff:ff:ff:ff
inet 10.10.3.5/28 brd 10.10.3.15 scope global eth0
    valid_lft forever preferred_lft forever
inet6 fd00:2003:4:1:a00:27ff:fe80:f0c2/64 scope global
    valid_lft 2591981sec preferred_lft 604781sec
inet6 fe80::a00:27ff:fe80:f0c2/64 scope link
    valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc p
n 1000
link/ether 08:00:27:35:0c:41 brd ff:ff:ff:ff:ff:ff
inet 10.0.3.15/24 brd 10.0.3.255 scope global eth1
    valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fe35:41/64 scope link
    valid_lft forever preferred_lft forever
4: eth0.0@eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500
1000
link/ether 08:00:27:f6:f0:c2 brd ff:ff:ff:ff:ff:ff
inet 10.10.3.37/28 brd 10.10.3.47 scope global eth0.0
    valid_lft forever preferred_lft forever
inet6 fd00:2003:4:1:a00:27ff:fe80:f0c2/64 scope global
    valid_lft 2591980sec preferred_lft 604780sec
```

Area 0.0.0.0, в шаблоне интерфейса указываем только bridge1 и vlan3 (для vlan2 IPv6 адресации нет).

Enabled	<input checked="" type="checkbox"/>		
Name	ospf-instance-1		
Version	3		
VRF	main		
Router ID	main		
Routing Table	▼		
Distance Default	▼		
connected	<input checked="" type="checkbox"/>	static	<input checked="" type="checkbox"/>
rip	<input type="checkbox"/>	ospf	<input checked="" type="checkbox"/>
Redistribute	▲	<input type="checkbox"/> bgp	<input type="checkbox"/> vpn

Enabled	<input checked="" type="checkbox"/>
Interfaces	bridge1
	vlan3
Enabled	<input checked="" type="checkbox"/>
Area	ospf-area-1
Name	ospf-area-1
Instance	ospf-instance-1
Area ID	0.0.0.0
Type	default

Посмотрим в OSPF LSA mt-01 (видно все зафиксированные устройства с маршрутами):

16 items											
		Instance	Area	Type	Originator	ID	Link	Link Insta... Id	Sequence	Age	
	SD	[ospf-instance-1]		external	10.10.3.33	0.0.0.0		0	80000001	201	
	SD	[ospf-instance-1]	ospf-area-1	link	10.10.3.33	0.0.0.1	%bridge1	0	80000001	97	
	SD	[ospf-instance-1]	ospf-area-1	link	10.10.3.33	0.0.0.2	%vlan3	0	80000001	97	
	SD	[ospf-instance-1]	ospf-area-1	intra-area-p	10.10.3.33	0.0.0.0		0	80000002	0	
	D	[ospf-instance-1]	ospf-area-1	link	10.10.3.34	0.0.0.1	%vlan3	0	80000001	5	
	SD	[ospf-instance-1]	ospf-area-1	router	10.10.3.33	0.0.0.0		0	80000002	0	
	SD	[ospf-instance-1]	ospf-area-1	network	10.10.3.33	0.0.0.2		0	80000003	0	
	D	[ospf-instance-1]	ospf-area-1	router	10.10.3.34	0.0.0.0		0	80000001	1	
	D	[ospf-instance-1]	ospf-area-1	link	10.10.3.34	0.0.0.2	%bridge1	0	80000001	5	
	SD	[ospf-instance-1]	ospf-area-1	network	10.10.3.33	0.0.0.1		0	80000003	0	
	SD	[ospf-instance-1]	ospf-area-1	intra-area-p	10.10.3.33	0.0.0.1		0	80000001	0	
	D	[ospf-instance-1]	ospf-area-1	link	10.10.3.35	0.0.0.1	%bridge1	0	80000001	2	
	D	[ospf-instance-1]	ospf-area-1	intra-area-p	10.10.3.35	0.0.0.0		0	80000001	2	
	D	[ospf-instance-1]	ospf-area-1	router	10.10.3.35	0.0.0.0		0	80000001	1	
	D	[ospf-instance-1]	ospf-area-1	link	10.10.3.35	0.0.0.2	%vlan3	0	80000001	2	
	SD	[ospf-instance-1]	ospf-area-1	intra-area-p	10.10.3.33	0.0.0.2		0	80000001	0	

Таблицы маршрутизации настроены, посмотрим в них: (для примера взят mt-01)

9 items				
		Dst. Address	Gateway	Distance
-	DAo	fd00:2003:4::/64	%vlan3	110
-	DAo	fd00:2003:4:0:a00:27ff:fe00::a00:27ff:fe0d:bc34%vlan3	fe80::a00:27ff:fe0d:bc34%vlan3	110
-	Dd	fd00:2003:4:1::/64		1
-	Do	fd00:2003:4:1::/64	%vlan3	110
-	DAC	fd00:2003:4:1::/64	%bridge1	
-	DAC	fe80::/64%bridge1	%bridge1	
-	DAC	fe80::/64%ether4	%ether4	
-	DAC	fe80::/64%vlan2	%vlan2	
-	DAC	fe80::/64%vlan3	%vlan3	

```

root@astra1:~# ping -6 fd00:2003:4:0:38df:e882:c95:6253
PING fd00:2003:4:0:38df:e882:c95:6253(fd00:2003:4:0:38df:e882:c95:6253) 56 data bytes
64 bytes from fd00:2003:4:0:38df:e882:c95:6253: icmp_seq=1 ttl=128 time=0.861 ms
64 bytes from fd00:2003:4:0:38df:e882:c95:6253: icmp_seq=2 ttl=128 time=0.787 ms
^C
--- fd00:2003:4:0:38df:e882:c95:6253 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.787/0.824/0.861/0.037 ms

```

astral -> mt-03

```

root@astra1:~# ping -6 fd00:2003:4:0:a00:27ff:fe0d:bc34
PING fd00:2003:4:0:a00:27ff:fe0d:bc34(fd00:2003:4:0:a00:27ff:fe0d:bc34) 56 data bytes
64 bytes from fd00:2003:4:0:a00:27ff:fe0d:bc34: icmp_seq=1 ttl=64 time=1.31 ms
64 bytes from fd00:2003:4:0:a00:27ff:fe0d:bc34: icmp_seq=2 ttl=64 time=0.672 ms
^C
--- fd00:2003:4:0:a00:27ff:fe0d:bc34 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.672/0.993/1.315/0.323 ms

```

host -> astra2

```

C:\Windows\System32>ping -6 fd00:2003:4:1:a00:27ff:fe40:3147

Обмен пакетами с fd00:2003:4:1:a00:27ff:fe40:3147 по с 32 байтами данных:
Ответ от fd00:2003:4:1:a00:27ff:fe40:3147: время<1мс
Ответ от fd00:2003:4:1:a00:27ff:fe40:3147: время<1мс
Ответ от fd00:2003:4:1:a00:27ff:fe40:3147: время<1мс
Ответ от fd00:2003:4:1:a00:27ff:fe40:3147: время<1мс

Статистика Ping для fd00:2003:4:1:a00:27ff:fe40:3147:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
        (0% потеря)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

```

3912 1630.2862... fd00:2003:4:1:1416:410c... fd00:2003:4:1:a00:27ff... ICMPv6	94 Echo (ping) request id=0x0001, seq=1
3913 1630.2863... fd00:2003:4:1:a00:27ff... fd00:2003:4:1:1416:410c... ICMPv6	94 Echo (ping) reply id=0x0001, seq=1
3930 1631.2885... fd00:2003:4:1:1416:410c... fd00:2003:4:1:a00:27ff... ICMPv6	94 Echo (ping) request id=0x0001, seq=2
3931 1631.2885... fd00:2003:4:1:a00:27ff... fd00:2003:4:1:1416:410c... ICMPv6	94 Echo (ping) reply id=0x0001, seq=2

Frame 3913: 94 bytes on wire (752 bits), 94 bytes captured (752 bits)	0000 0a 00 27 00 00
Ethernet II, Src: PcsCompu_40:31:47 (08:00:27:40:31:47), Dst: 0a:00:27:00:00:0d (0a:00:27:00:00:0d)	0010 e4 d6 00 28 3a
Internet Protocol Version 6, Src: fd00:2003:4:1:a00:27ff:fe40:3147, Dst: fd00:2003:4:1:1416:410c	0020 27 ff fe 40 31
Internet Control Message Protocol v6	0030 41 0c 1c b4 59
	0040 63 64 65 66 67

13. На виртуальной машине astra2 проверим настройки DNS клиента в файле /etc/resolv.conf: сейчас там указан домашний маршрутизатор, к которому подключен хост.

GNU nano 2.7.4	Файл: /etc/resolv.conf
nameserver 192.168.10.1	

Изменим файл так, чтобы новыми серверами стали DNS-сервера Google:

GNU nano 2.7.4	Файл: /etc/resolv.conf
domain lan	
search lan	
nameserver 8.8.8.8	
nameserver 8.8.4.4	

Перезапустим систему DNS:

```

root@astra2:~# systemctl restart systemd-resolved.service

```

Убедимся, что запросы по умолчанию передаются на DNS с адресом 8.8.8.8: пропишем в терминале команду “`systemd-resolve –status`”

```
Global
DNS Servers: 8.8.8.8
               8.8.4.4
DNS Domain: lan
```

14. Используя консольную утилиту nslookup, загруженную командой “`apt-get install dnsutils`”, с узла astra2, найдём информацию о DNS-зоне csc.sibsutis.ru:

```
root@astra2:~# nslookup -q=any csc.sibsutis.ru
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
csc.sibsutis.ru
    origin = ns.csc.sibsutis.ru
    mail addr = root.csc.sibsutis.ru
    serial = 20
    refresh = 10800
    retry = 900
    expire = 604800
    minimum = 86400
csc.sibsutis.ru nameserver = ns.csc.sibsutis.ru.
csc.sibsutis.ru mail exchanger = 10 mx.yandex.net.
csc.sibsutis.ru text = "MS=ms84877494"
csc.sibsutis.ru text = "v=spf1 redirect=_spf.yandex.net"
csc.sibsutis.ru text = "yandex-verification: fd2cf5e61ab13a5"
Name:   csc.sibsutis.ru
Address: 91.196.245.193
```

О6 IPv4 имени ans.csc.sibsutis.ru:

```
root@astra2:~# nslookup ans.csc.sibsutis.ru
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   ans.csc.sibsutis.ru
Address: 1.1.1.1
```

Обо всех IP адресах, найденных для домена mail.ru:

```
root@astra2:~# nslookup mail.ru
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   mail.ru
Address: 94.100.180.200
Name:   mail.ru
Address: 217.69.139.202
Name:   mail.ru
Address: 217.69.139.200
Name:   mail.ru
Address: 94.100.180.201
Name:   mail.ru
Address: 2a00:1148:db00:0:b0b0::1
```

IPv4 адрес домена mail.ru:

```
root@astra2:~# nslookup -q=A mail.ru
Server:      8.8.8.8
Address:     8.8.8.8#53

Non-authoritative answer:
Name:   mail.ru
Address: 217.69.139.200
Name:   mail.ru
Address: 94.100.180.201
Name:   mail.ru
Address: 94.100.180.200
Name:   mail.ru
Address: 217.69.139.202
```

Все задания расчётно-графической работы выполнены успешно.

:

1. Измените настройки STP таким образом, чтобы коммутатор Mikrotik-4 из резервного перешел в состояние рабочего.

Для изменения состояния порта коммутатора Mikrotik-4 в STP на «рабочий», нужно выполнить команду изменения приоритета порта, а затем активировать его: /interface bridge port set [find interface=имя_порта] priority=8192

2. Модель открытых систем OSI/ISO. Зачем она используется? Какие функции выполняются на уровнях 1 и 2?

Модель OSI (Open Systems Interconnection) используется для стандартизации процессов связи. На уровне 1 (физический) происходит передача битов по кабелям, а на уровне 2 (канальный) осуществляется управление доступом к среде передачи и проверка на ошибки.

3. Физический уровень технологии Ethernet. Какие физические среды используются для передачи сигнала? Как кодируется 0 и 1 в этих средах?

Физические среды Ethernet включают витую пару, коаксиальные кабели и оптоволокно. Кодирование 0 и 1 осуществляется с помощью различных сигналов (например, в витой паре - с помощью напряжения).

4. Коммутация Ethernet. Как устроены разъемы используемые для подключения витой пары и оптоволокна?

Разъемы для витой пары (RJ-45) и оптоволокна (LC, SC) отличаются количеством контактов и формой пазов для правильной установки.

5. Коммутация Ethernet. Какие стандарты существуют для расположения контактов в разъемах для подключения Ethernet по витой паре? В чем их разница? Почему синяя и зеленые пары в стандарте 568А (или оранжевая и синяя пары в стандарте 568В) расположены не последовательно друг за другом?

Стандарты T568A и T568B для витой пары определяют расположение контактов. Они отличаются тем, что порядок пар различается, чтобы минимизировать crosstalk. Синяя и зеленая пары не расположены последовательно для избежания помех.

6. Коммутация Ethernet. Какая максимальная длина кабеля витой пары может быть при подключении по технологии Ethernet? Какая максимальная длина оптоволоконного кабеля может быть при подключении по технологии Ethernet?

Максимальная длина витой пары в Ethernet — 100 метров, максимальная длина оптоволоконного кабеля может достигать нескольких километров, в зависимости от типа волокна и технологий.

7. Коммутация Ethernet. Возможно ли организация сети по технологии Ethernet без использования кабельного соединения? Если да, то какие физические среды могут быть использованы?

Да, возможна организация сети по технологии Ethernet без кабелей с использованием беспроводных технологий (например, Wi-Fi).

8. Для чего используется система VirtualBox?

VirtualBox используется для создания и управления виртуальными машинами, что позволяет тестировать ОС и программы без влияния на основную систему.

9. Какие два типа окон присутствуют в графическом интерфейсе VirtualBox? В чем из отличия?

В графическом интерфейсе VirtualBox существуют два типа окон: главное окно (управление виртуальными машинами) и окно консоли (интерфейс виртуальной машины). Главное окно отображает все доступные ВМ, а консоль предоставляет доступ к работающей ВМ.

10. Форматы файлов виртуальных носителей. Какие форматы поддерживаются в VirtualBox?

VirtualBox поддерживает форматы файлов виртуальных носителей, такие как VDI (VirtualBox Disk Image), VMDK (VMware Disk), VHD (Virtual Hard Disk) и другие.

11. Типы доступа к виртуальным носителям

Типы доступа к виртуальным носителям в VirtualBox могут включать «с множественным подключением» (multiple connections) и «неизменяемый» (immutable).

С множественным подключением: это означает, что несколько виртуальных машин могут одновременно использовать один и тот же виртуальный носитель. Изменения, сделанные одной машиной, сохраняются и видны другим.

Неизменяемый: здесь носитель можно использовать только для чтения. Все изменения попадают в отдельный слой, и оригинал остается нетронутым. Это полезно для тестирования и сохранения состояния.

12. Коммутация сетей в VirtualBox

VirtualBox поддерживает несколько типов физических соединений:

NAT: виртуальная машина использует сеть хоста для доступа в интернет.

Сетевая мостовая связь: виртуальная машина напрямую подключается к сети хоста, как будто она физическое устройство.

Внутренняя сеть: машины могут обмениваться данными только между собой в рамках одной внутренней сети.

Сетевой шифратор (Host-only): виртуальная машина общается с хостом и другими ВМ, но не имеет доступа к внешней сети.

13. Режимы запуска виртуальных машин

Режимы запуска виртуальных машин:

Интерактивный режим: виртуальная машина запущена в окне, и пользователь может взаимодействовать с ней.

Фоновый режим: ВМ работает в фоновом режиме, без графического интерфейса.

Параметры управления осуществляются через командную строку или другие инструменты.

Консоль: это интерфейс, через который пользователь может управлять виртуальной машиной. В работах с консолью важно понимать, что нужно вводить команды точно, чтобы избежать ошибок.

14. HostKey в VirtualBox

HostKey — это сочетание клавиш, используемое для переключения между виртуальной машиной и хост-операционной системой. Это нужно, чтобы легко вернуть управление на хост, не останавливая ВМ.

15. Функции Wireshark

Wireshark выполняет множество функций, включая:

Захват пакетов с сетевого интерфейса.

Анализ и декодирование данных протоколов.

Просмотр информации о сетевых соединениях.

Фильтрация и сортировка трафика.

16. Изменение масштаба отображения в Wireshark

Масштаб отображения в Wireshark можно изменить с помощью колесика мыши или сочетаний клавиш Ctrl и +/- . Также можно использовать меню для изменения масштаба.

17. Включение/отключение разрешения имен

В Wireshark можно включить или отключить разрешение имен в меню "View" > "Name Resolution", где можно выбрать соответствующие параметры.

18. Сохранение и открытие захваченного потока пакетов

Чтобы сохранить поток пакетов в Wireshark, используйте "File" > "Save As...". Чтобы открыть ранее сохранённый файл, выберите "File" > "Open...".

19. Редактирование сохранённого потока пакетов

Wireshark не поддерживает редактирование пакетов непосредственно, но с помощью фильтров можно создать новый файл с нужными пакетами, используя "File" > "Export Specified Packets..." и задав нужные параметры фильтрации.

20. Фильтрация пакетов

Чтобы отфильтровать пакеты по протоколу DHCP, используйте фильтр: **bootp**. Для HTTP - фильтр: **http**.

21. Как в Wireshark создать типовой фильтр? Как его использовать? Чтобы создать типовой фильтр, вы можете использовать панель фильтров в верхней части интерфейса Wireshark. Введите ваше условие (например, **http**, **ip.addr == 192.168.1.1** и др.) и нажмите Enter. Фильтр будет применен к захваченным пакетам.

22. Как в Wireshark настроить интерфейс так, чтобы в процессе захвата потока пакетов курсор автоматически помещался на последний полученный пакет?

Перейдите в "View" > "Auto Scroll" и выберите "Scroll to Bottom on Packet Arrival". Это позволит вам автоматически перемещаться к последнему пакету при их получении.

23. Как в интерфейсе включить/отключить оформление цветом логически связанных пакетов? Перейдите в "View" > "Coloring Rules". Вы можете включить или отключить правила покраски, а также дополнительно изменять их.

24. Как в интерфейсе Wireshark посмотреть содержимое пакета? Можно ли увидеть вложенные составляющие в соответствии с моделью OSI/ISO? Выберите пакет в списке и посмотрите на содержащиеся в нем данные в нижней панели. Здесь вы сможете увидеть вложенные протоколы в виде дерева, что соответствует модели OSI.

25. Что такое МАС адрес? Зачем он используется? МАС-адрес (Media Access Control) — это уникальный идентификатор сетевого интерфейса для сетевых устройств. Он используется для идентификации устройства в локальной сети.

26. Определена ли какая-либо структура МАС-адреса? Что будет, если эту структуру не соблюдать? МАС-адрес состоит из 48 бит (6 байт), часто записываемых в виде шестнадцатеричных чисел, разделенных двоеточиями. Если структура не соблюдается, устройства могут не распознать адрес, что приведет к проблемам с соединением.

27. Допускается ли в одном сегменте сети два сетевых интерфейса с одинаковым МАС-адресом? Нет, это вызывает конфликты. Две сетевые карты с одинаковыми МАС-адресами в одном узле могут вызывать проблемы с определением пакетов в локальной сети.

28. Что такое «широковещательный» МАС-адрес? Зачем он используется? Есть ли еще какие-то служебные МАС-адреса? Широковещательный МАС-адрес — это **FF:FF:FF:FF:FF**, он используется для рассылки сообщений всем устройствам в сети. Существуют и другие специальные адреса, такие как мультикастовые адреса.

29. Как определить МАС адреса сетевых интерфейсов на маршрутизаторе Mikrotik? В операционной системе AstraLinux? На Mikrotik используйте команду в терминале: **/interface print**. В AstraLinux можно использовать команду **ifconfig** или **ip link**.

30. Возможно ли изменить эти МАС адреса? Если да, то как это сделать? Да, МАС-адреса можно изменить в настройках сетевого интерфейса. В Mikrotik это делается через интерфейс пользователя или команды, в Linux можно использовать **ifconfig eth0 hw ether 00:11:22:33:44:55**.

31. Что такое IP адрес? Как устроен IP адрес версии 4? Десятично-точечная нотация. IP адрес — это уникальный идентификатор, который назначается каждому устройству в сети, позволяющий отправлять и получать данные.

IP адреса версии 4 (IPv4) состоят из 32 бит, что делит адрес на четыре октета (по 8 бит в каждом). Каждый октет записывается в десятичной форме и разделяется точками, например: **192.168.1.1**. Каждый октет может принимать значения от 0 до 255.

32. Структура пакета сетевого уровня для IPv4. Какие поля содержит?

Пакет IPv4 состоит из заголовка и полезной нагрузки. Заголовок включает следующие поля:

Версия (4 бита)
Длина заголовка (4 бита)
Услуга (8 бит)
Длина пакета (16 бит)
Идентификатор (16 бит)
Флаги (3 бита)
Смещение фрагмента (13 бит)
Время жизни (TTL, 8 бит)
Протокол (8 бит)
Контрольная сумма (16 бит)
IP-адрес источника (32 бита)
IP-адрес назначения (32 бита)
Дополнительные поля (если необходимо)

33. Пространство адресов IPv4. Группирование адресов. Классовая и бесклассовая адресация.

IPv4 использует 32-битные адреса, что дает 4,3 миллиарда уникальных адресов. Адреса могут быть сгруппированы в классы (A, B, C, D, E), и каждая группа имеет свои правила назначения.

Классовая адресация: определяет адреса на основе первых битов.

Бесклассовая адресация (CIDR): более гибкий подход, где адреса представляются с префиксом, например, /24.

34. Что такое маска сети и как она используется?

Маска сети — это 32-битное число, которое определяет, какая часть IP-адреса относится к сети, а какая — к устройству. Например, для адреса **192.168.1.0** и маски **255.255.255.0** адрес сети — это **192.168.1.0**.

Широковещательный адрес используется для отправки данных всем устройствам в сети. Нельзя назначить адрес сети или широковещательный адрес на узел.

35. Как вычислить маску, если известно сколько адресов должно быть в подсети?

Чтобы вычислить маску:

Определите количество необходимых адресов (N).

Найдите наименьшую степень двойки, которая больше или равна N. Например, 32 адреса требуют маску /27 ($2^5 = 32$).

Если нужно уменьшить или увеличить количество подсетей, изменение маски (префикса) возможно.

36. VLSM и CIDR - что это?

VLSM (Variable Length Subnet Mask) позволяет использовать маски различной длины для разных подсетей в одной сети.

CIDR (Classless Inter-Domain Routing) - бесклассовая адресация, которая позволяет более эффективно использовать адресное пространство.

Маска вида **1.2.3.4** — допустима, но чаще всего используются маски вида **255.255.255.0**. Запись вида **адрес/длина_префикса** указывает, сколько бит используется для обозначения сети.

37. Как связаны сетевой адрес и MAC-адрес? Протокол ARP.

Протокол ARP (Address Resolution Protocol) используется для преобразования IP-адресов в MAC-адреса. Сообщения ARP отправляются в одноадресном режиме (запросы) и многоадресном режиме (ответы).

Структура пакета ARP включает:

Тип аппарата

Тип протокола

Длина адреса

Операция (запрос/ответ)

MAC и IP-адреса источника и назначения.

38. Как принимается решение, какой MAC адрес использовать?

MAC-адреса определяются устройствами в сети. Специальные MAC-адреса используются для широковещательной передачи (например, FF:FF:FF:FF:FF:FF) или многоадресных рассылок. Примеры пакетов могут включать такие адреса в заголовках Ethernet.

39. Что произойдет, если в сети будут двум разным устройствам назначен одинаковый IPv4 адрес?

Это приведёт к конфликту адресов, и устройства не смогут правильно обмениваться данными, что вызовет проблемы в сетевом взаимодействии.

40. Как посмотреть таблицу разрешенных IP адресов в устройствах?

Mikrotik: используйте команду /ip arp print в терминале.

Linux: команду arp -n или ip neighbor show.

Windows: команду arp -a в командной строке.

41. Можно ли добавить статические записи в таблицу MAC адресов? Если можно, то зачем это может потребоваться?

Да, статические записи можно добавлять в таблицу MAC-адресов. Это может потребоваться для следующих целей:

Устойчивость: Закрепление MAC-адреса за определённым портом, чтобы избежать его удаления из таблицы при изменениях в сети.

Безопасность: Защита от атак типа "ARP spoofing" путем фильтрации только заранее известных MAC-адресов.

Управление трафиком: Повышение производительности, так как необходимость в динамической обучении MAC-адресов уменьшается.

43. Как настраивается статическая адресация IPv4 в маршрутизаторе Mikrotik?

CLI:

```
/ip address add address=192.168.1.10/24 interface=ether1
```

Web-интерфейс:

Перейдите в раздел "IP" -> "Addresses".
Нажмите на "+" для добавления нового адреса.
Ведите IP-адрес и выберите интерфейс.
Нажмите "OK".

WinBox:

Откройте WinBox и подключитесь к маршрутизатору.
Перейдите в "IP" -> "Addresses".
Нажмите на "+" для добавления нового адреса.
Ведите необходимые данные и нажмите "OK".

44. Как вывести все назначенные IPv4 адреса на интерфейсах маршрутизатора Mikrotik?

В CLI:

```
/ip address print
```

Допускается ли назначение на один интерфейс нескольких адресов IPv4? Да, можно назначить на один интерфейс несколько адресов.

Должны ли быть это адреса из одного диапазона? Нет, адреса могут быть из разных диапазонов.

А из одного диапазона на разные интерфейсы? Да, это также допускается.

45. Как удалить назначенный IPv4 адрес в маршрутизаторе Mikrotik? А как изменить адрес? Маску?

Удаление адреса:

```
/ip address remove [find address=192.168.1.10]
```

Изменение адреса или маски:

```
/ip address set [find address=192.168.1.10] address=192.168.1.20/24
```

47. Как настраивается статическая адресация IPv4 в операционной системе AstraLinux?

В AstraLinux назначение IP-адреса можно выполнить через консоль. Команда для установки статического IP:

```
ip addr add 192.168.1.10/24 dev eth0
```

48. Как вывести все назначенные IPv4 адреса на сетевых интерфейсах AstraLinux?

Для вывода всех назначенных адресов:

```
ip addr show
```

49. Допускается ли назначение на один интерфейс нескольких адресов IPv4?

Да, это допускается.

Должны ли быть это адреса из одного диапазона? Нет, они могут быть из разных диапазонов.

Допускается ли назначить адреса из одного диапазона на разные интерфейсы? Да, это также возможно.

50. Как удалить назначенный IPv4 адрес в AstraLinux?

Для удаления адреса:

```
ip addr del 192.168.1.10/24 dev eth0
```

52. Протокол ICMP

ICMP (Internet Control Message Protocol) используется для передачи сообщений об ошибках и другой информации, касающейся IP-сетей. Основные типы сообщений ICMP включают:

Echo Request (Запрос эха): используется утилитой ping для проверки доступности хоста.

Echo Reply (Ответ на эхо): ответ на запрос эха.

53. Структура пакета ICMP

Структура пакета ICMP включает следующие поля:

Type: тип сообщения (например, 8 для echo request, 0 для echo reply).

Code: код уточняющий тип сообщения.

Checksum: контрольная сумма для обнаружения ошибок.

Identifier: идентификатор запроса.

Sequence Number: номер последовательности запроса.

Примеры пакетов можно захватить с помощью Wireshark или аналогичных инструментов.

55. Принцип работы сетевого коммутатора

Сетевой коммутатор работает на уровне канального уровня (Layer 2) модели OSI. Он пересыпает данные между соединенными устройствами, используя таблицы MAC-адресов для определения, куда отправлять пакеты. Главное отличие от концентратора (hub) заключено в том, что коммутатор направляет пакеты только к нужному порту, а концентратор рассыпает их на все порты.

56. Таблица коммутации пакетов

Таблица коммутации содержит записи о MAC-адресах, связанных с каждым портом коммутатора. Она позволяет коммутатору эффективно направлять пакеты конкретному устройству, сокращая количество ненужного трафика в сети. Применение таблицы было заметно в различных практических заданиях, где сеть демонстрировала более высокую производительность.

57. Таблица коммутации и специальные MAC адреса

Специальные MAC-адреса, такие как широковещательные (ff:ff:ff:ff:ff:ff) и многоадресные, обрабатываются коммутатором иначе. Широковещательные пакеты рассыпаются на все порты, а многоадресные могут направляться на несколько определенных портов, в зависимости от группы, к которой относятся.

58. Коллизия

Коллизия происходит, когда два устройства пытаются одновременно отправить данные в сеть. В технологии Ethernet (CSMA/CD) разрешение коллизий происходит путем обнаружения конфликта и временной задержки отправки пакетов. **Домен коллизий** — это область сети, где могут происходить коллизии. Например, все устройства, подключенные к одному концентратору, образуют домен коллизий.

59. Широковещательный домен

Широковещательный домен — это область сети, в которой широковещательные сообщения могут быть приняты всеми устройствами. Он связан с доменом коллизий,

так как в одном широковещательном домене могут происходить коллизии, когда пакеты передаются по сетям с общими соединениями.

60. Разные диапазоны адресов в одном широковещательном домене

Как правило, в одном широковещательном домене не рекомендуется смешивать адреса из разных подсетей, так как это может привести к проблемам с маршрутизацией. Широковещательные сообщения отправляются всем устройствам в домене, и если они находятся в разных подсетях, это может вызвать путаницу и проблемы с сетевым трафиком.

62. Динамическое конфигурирование сетевых интерфейсов. Протокол DHCP, технология APIPA?

DHCP (Dynamic Host Configuration Protocol) — это сетевой протокол, который используется для автоматического назначения IP-адресов и других параметров конфигурации сетевых интерфейсов в компьютерной сети. **APIPA (Automatic Private IP Addressing)** — это технология, которая позволяет устройствам автоматически назначать себе IP-адреса в диапазоне 169.254.0.1 - 169.254.255.254, если DHCP-сервер недоступен.

63. Как происходит конфигурирование сетевого интерфейса по APIPA.

Если устройство не может получить IP-адрес через DHCP, оно автоматически выбирает случайный адрес из диапазона APIPA. Устройство проверяет, не используется ли этот адрес в сети. Если адрес свободен, он назначается устройству.

64. Типы сообщений в протоколе DHCP.

Существует несколько типов сообщений:

DHCPDISCOVER — запрос на получение IP-адреса.

DHCPOFFER — предложение IP-адреса от DHCP-сервера.

DHCPREQUEST — запрос на подтверждение IP-адреса.

DHCPCACK — подтверждение назначения IP-адреса клиенту.

DHCPNAK — отказ в назначении IP-адреса.

Дополнительно, **DHCPRELEASE**, **DHCPIINFORM**.

Режим передачи: Используется широковещательный режим для первых сообщений и одноадресный для подтверждения.

65. Возможна ли передача DHCP пакетов в одноадресном режиме?

Да, DHCP-пакеты могут передаваться в одноадресном режиме, когда клиент уже знает свой IP-адрес и отправляет запрос на конкретный DHCP-сервер для получения

параметров конфигурации. Это может использоваться в случае, если клиент получает адрес от сервера.

66. Что будет, если в сети установить два узла, на которых запустить DHCP сервер?

Если в сети присутствуют два DHCP-сервера, это может вызвать конфликты IP-адресов, так как оба сервера могут назначать одни и те же адреса разным клиентам, что приведет к проблемам с соединением и сетевым конфликтам.

67. Каковы условия конфигурирования DHCP сервера в сети?

Должен быть доступен IP-адрес для DHCP-сервера и диапазон адресов для раздачи. Необходимо настроить параметры, такие как шлюз, DNS-сервер и время аренды адресов.

DHCP-сервер должен быть подключен к сети, где клиенты могут его обнаружить.

68. Как организовать работу DHCP в сети без физического DHCP сервера?

Используется **DHCP Relay Agent**. Это промежуточное устройство, которое перенаправляет DHCP-запросы от клиентов к серверу, находящемуся в другой подсети. Один DHCP-сервер может обслуживать несколько подсетей через реле агентов.

69. Сетевой адрес IPv6. Структура.

IPv6 адрес состоит из 128 бит, записывается в виде восьми групп по 16 бит, разделенных двоеточиями (например, **2001:0db8:85a3:0000:0000:8a2e:0370:7334**).

Типы адресов:

Уникаст (Unicast) — для одного получателя.

Мульти cast (Multicast) — для группы получателей.

Эддресс любой (Anycast) — для ближайшего получателя.

Префикс — это часть адреса, которая используется для обозначения сети.

Способы сокращения записи: Например, **2001:0db8:0000:0000:0000:0000:0001** можно упростить до **2001:db8::1**.

70. Link-local адреса. Зачем используются?

Link-local адреса используются для связи устройств в одной сети без необходимости маршрутизации. Эти адреса имеют диапазон **FE80::/10** и могут использоваться для автоматического конфигурирования и соседского обнаружения.

71. Формирование интерфейсной части link-local адреса и EUI-64

Link-local адреса в IPv6 формируются на основе MAC-адреса устройства. Стандарт EUI-64 позволяет преобразовать 48-битный MAC-адрес в 64-битный идентификатор интерфейса. Этот процесс включает вставку **FFFF** в середину MAC-адреса и изменение одного бита (7-й бит) для создания уникального идентификатора.

Пример: Если MAC-адрес устройства: **00:1A:2B:3C:4D:5E**, то интерфейсная часть будет:

Изменяем: **00:1A:2B** на **02:1A:2B**.

Вставляем **FFFF**: **021A:2BFF:FE3C:4D5E**.

Получаем: **fe80::21a:2bff:fe3c:4d5e**.

72. Проверка связи с узлами через link-local адреса и идентификатор интерфейса

Связь с узлами можно проверить, используя утилиту **ping** с указанием link-local адреса. Однако нужно указывать идентификатор интерфейса, например, **ping fe80::21a:2bff:fe3c:4d5e%eth0**. Идентификатор интерфейса указывает, через какой сетевой интерфейс отправляется пакет.

73. Unique Local Unicast IPv6 адрес

Диапазон адресов: **fc00::/7**.

Назначение: Эти адреса предназначены для использования в частных сетях, подобно приватным IPv4-адресам. Они не маршрутизируются в интернете и могут использоваться для внутренней связи.

74. Global Unicast IPv6 адрес

Диапазон адресов: **2000::/3**.

Назначение: Эти адреса уникальны и могут маршрутизироваться в интернете, что позволяет устройствам в глобальной сети устанавливать соединения.

75. Специальные диапазоны адресов IPv6

::1: Мультикаст адрес для локального устройства (loopback).

::/128: Указывает на несуществующий адрес.

FF00::/8: Мультикаст адреса.

::ffff:0:0/96: Для совместимости с IPv4.

IPv6 имеет несколько специальных диапазонов адресов, каждый из которых имеет свое назначение. Вот основные из них:

Loopback адрес:

- **Адрес:** ::1
- **Назначение:** Используется для самопроверки устройства. Это аналог адреса 127.0.0.1 в IPv4.

Сылочный адрес:

- **Сначала 80 нулей:** ::FFFF:0:0/96
- **Назначение:** позволяет использованию IPv4-адресов в сетях IPv6, предоставляя совместимость для IPv4.

Мультикастовые адреса:

- **Диапазон:** FF00::/8
- **Назначение:** Используются для соединений мультикастом, позволяя отправлять пакеты группе узлов вместо одного конкретного.

Универсальные локальные адреса:

- **Диапазон:** FC00::/7
- **Назначение:** Частные адреса, используемые в локальных сетях. Эти адреса не маршрутизируются в Интернете.

Тестовые и резервные адреса:

- **Пример адреса:** 2001:DB8::/32
- **Назначение:** Резервированы для документации и примеров, чтобы избежать путаницы с реальными адресами.

Unspecified address:

- **Адрес:** ::
- **Назначение:** Используется для указания "неопределенного" адреса, когда адрес не известен или не применяется.

76. Протокол NDP (Neighbor Discovery Protocol)

Типы сообщений включают:

Router Solicitation (RS): Запрос на информацию о маршрутизаторах.

Router Advertisement (RA): Ответ на RS, содержащий информацию о маршрутизаторах.

Neighbor Solicitation (NS): Запрос о MAC-адресе устройства.

Neighbor Advertisement (NA): Ответ на NS.

77. Определение соседа с помощью NDP

С помощью сообщения Neighbor Solicitation (NS) можно узнать MAC-адрес устройства. Пример пакета может включать запрашиваемый IP-адрес и MAC-адрес отправителя, отправленный в multicast.

78. Статическая конфигурация IPv6 на маршрутизаторе Mikrotik

CLI:

Задать адрес: `/ipv6 address add address=2001:db8::1/64 interface=ether1`

Изменить: `/ipv6 address set [find address=2001:db8::1] address=2001:db8::2/64`

Удалить: `/ipv6 address remove [find address=2001:db8::2]`.

Web/WinBox: Интерфейс предоставляет форму для внесения изменений.

79. Статическая конфигурация IPv6 в AstraLinux

Задать адрес: В файле конфигурации сети `/etc/network/interfaces` добавьте строку.
`Plain
iface eth0 inet6 static
address 2001:db8::1
netmask 64`

Изменить/Удалить: Редактируйте этот файл соответствующим образом и перезапустите сетевой интерфейс.

80. Использование NDP при статической конфигурации IPv6

Протокол NDP автоматически обновляет таблицы ARP, когда в сети появляются новые устройства. Таким образом, даже при статической конфигурации, оставшиеся устройства смогут правильно определять MAC-адреса, обеспечивая корректную маршрутизацию пакетов.

81. SLAAC: Зачем используется? Как работает?

SLAAC (Stateless Address Autoconfiguration) используется для автоматической конфигурации IPv6-адресов, позволяя устройствам самостоятельно генерировать свои адреса без необходимости в DHCP-сервере. Он работает путём получения сетевых префиксов от маршрутизаторов, а затем по этому префиксу и MAC-адресу генерации уникального адреса.

82. SLAAC и протокол NDP

SLAAC использует Neighbor Discovery Protocol (NDP) для автоконфигурации адресов. Основные сообщения включают:

Router Solicitation (RS): Устройства запрашивают информацию о маршрутизаторах.

Router Advertisement (RA): Маршрутизаторы сообщают свои настройки, включая префиксы. Пример: устройство отправляет RS, а в ответ получает RA с префиксом и временем жизни.

83. Как долго сохраняются автоматически назначенные IPv6?

Автоматически назначенные адреса сохраняются до тех пор, пока устройство активно в сети. Информация о префиксах обычно распространяется каждые 200 секунд. Да, могут одновременно использоваться статически назначенные адреса и адреса, полученные по SLAAC.

84. MAC и IPv6 в NDP

В процессах NDP используется MAC-адрес для формирования IPv6-адреса через EUI-64, а также IPv6-адреса для обмена сообщениями. DAD (Duplicate Address Detection) проверяет, не занят ли уже адрес действующим устройством, отправляя Neighbor Solicitation и ожидая ответа.

85. Один IPv6 адрес на нескольких интерфейсах?

Один IPv6-адрес нельзя назначить сразу многим интерфейсам на одном узле, так как это приведет к конфликтам в маршрутизации. Однако можно настроить адреса на разных интерфейсах, но они должны быть уникальными.

86. Протокол ICMPv6

ICMPv6 — это расширение ICMP для IPv6. Он включает новые типы сообщений, такие как Router Solicitation и Router Advertisement, а также Neighbor Solicitation и Neighbor Advertisement. У пакетов ICMPv6 более сложная структура, включающая заголовки для идентификации типа сообщения и соответствующих данных.

87. DHCPv6: Типы сообщений, структура пакета

DHCPv6 включает типы сообщений, такие как Relay-Forward, Relay-Reply, Solicitation, Advertisement, Request и Reply. Структура пакета включает заголовок с типами сообщений и параметры, такие как идентификаторы клиентских и серверных сообщений.

88. Связь DHCP и SLAAC

DHCP и SLAAC могут использоваться вместе. SLAAC автоматически настраивает адреса, а DHCPv6 может использоваться для получения других параметров конфигурации, таких как DNS-серверы.

89. Настройка DHCP на маршрутизаторах Mikrotik: DHCP-Client

На Mikrotik DHCP-клиент настраивается через интерфейс или терминал. Это позволяет маршрутизатору получать адрес и сетевые настройки от DHCP-сервера в сети для доступа к интернету.

90. Настройка DHCP на маршрутизаторах Mikrotik: DHCP-Server

DHCP-сервер на маршрутизаторе Mikrotik предоставляет IP-адреса и настройки клиентам в локальной сети. Он упрощает управление сетевыми адресами и позволяет автоматизировать процесс подключения новых устройств.

91. Настройка DHCP в AstraLinux. DHCP-Client.

DHCP-клиент в AstraLinux настраивается обычно через конфигурационный файл `/etc/dhcp/dhclient.conf`. Вам нужно будет включить соответствующие параметры для получения IP-адреса автоматически.

92. Настройка DHCP в AstraLinux. DHCP-Server.

Для настройки DHCP-сервера в AstraLinux необходимо установить пакет `isc-dhcp-server`, настроить файл конфигурации `/etc/dhcp/dhcpd.conf`, определив диапазон адресов, время аренды и другие параметры.

93. DHCPv6 и NDP. Используются совместно?

Да, DHCPv6 и NDP (Neighbor Discovery Protocol) используют совместно, чтобы обеспечить автоматическую конфигурацию IP-адресов и управление соседями в IPv6-сетях. NDP помогает в обнаружении других устройств в сети, а DHCPv6 — в динамической передаче IP-адресов.

94. Что такое сетевой маршрут? Таблица маршрутов? Сколько таблиц маршрутов может быть на одном узле?

Сетевой маршрут — это путь, по которому передаются данные от одного узла к другому. Таблица маршрутов — это структура данных, содержащая маршруты к различным сетям. На одном узле может быть несколько таблиц маршрутов, особенно в сложных сетевых конфигурациях.

95. Технология CIDR. Как и зачем она используется в маршрутизаторах?

CIDR (Classless Inter-Domain Routing) позволяет более эффективно управлять адресным пространством, используя маски подсети переменной длины. Это уменьшает количество записей в таблицах маршрутизации и позволяет лучше использовать IP-адреса.

96. Статическая маршрутизация. Процесс определения маршрута для передачи пакета. Маршрут «по умолчанию». Политика маршрутизации.

Статическая маршрутизация предполагает ручное определение маршрутов в таблице маршрутизации. Маршрут "по умолчанию" используется, когда нет других маршрутов для передачи пакетов. Политика маршрутизации — это набор правил, определяющий, как выбирать маршруты.

97. Алгоритм поиска проблем с маршрутизацией.

Проверка подключения к шлюзу.

Проверка таблицы маршрутизации.

Тестирование ping для конечных устройств.

Анализ трассировки маршрута (traceroute).

98. Как получить информацию о таблице(ах) маршрутизации для IPv4 и IPv6 на маршрутизаторе Mikrotik, в операционной системе AstraLinux.

На Mikrotik: используйте команду `/ip route print` для IPv4 и `/routing/ipv6/route/print` для IPv6.

В AstraLinux: используйте `ip route show` для IPv4 и `ip -6 route show` для IPv6.

99. Динамическая маршрутизация. Зачем используется? Виды протоколов динамической маршрутизации.

Динамическая маршрутизация автоматически обновляет таблицы маршрутизации и адаптируется к изменениям сети. Основные виды протоколов: RIP, OSPF, EIGRP, BGP.

100. Протокол динамической маршрутизации RIP. Принцип работы. Версии протокола. Структура используемых пакетов.

RIP использует алгоритм "ближайшего соседа", обновляя таблицы маршрутизации каждые 30 секунд. Версии: RIP v1 и RIP v2. Структура пакета включает адрес назначения, метрику и информацию о маршруте.

101. Протокол динамической маршрутизации OSPF. Принцип работы. Версии протокола. Структура используемых пакетов. Понятие «область обмена маршрутами».

OSPF использует алгоритм Dijkstra для нахождения кратчайшего пути. Области маршрутов помогают делить большую сеть на подъёмы, уменьшая нагрузку. Версии: OSPFv2 и OSPFv3.

102. Интеграция данных между протоколами RIP и OSPF. Возможна ли? Приведите пример применения такой интеграции.

Интеграция возможна через маршрутизаторы, поддерживающие оба протокола. Например, можно настроить RIP для обмена маршрутами с OSPF на границе двух сетей.

103. Настройки ядра операционной системы Linux. Переменные net.ipv4.ip_forward и net.ipv4.conf.all.rp_filter. Зачем нужны? Какие ещё переменные используются?

`net.ipv4.ip_forward` включает пересылку пакетов между интерфейсами.
`net.ipv4.conf.all.rp_filter` усиливает безопасность, предотвращая подделку IP-адресов. Используются и другие переменные, как `net.ipv4.conf.all.accept_redirects`.

104. Что такое фильтрация сетевых пакетов? Зачем используется? Приведите примеры.

Фильтрация сетевых пакетов — это процесс анализа и фильтрации сетевых данных для блокировки или разрешения трафика. Примеры: блокировка специфических IP-адресов, разрешение пакетов только для определенных портов.

105. Как настроить фильтрацию пакетов в маршрутизаторах Mikrotik.

Используйте Winbox или командной строки для создания правил фильтрации в разделе IP > Firewall.

106. Как настроить фильтрацию пакетов в операционной системе AstraLinux?

Используйте `iptables` или `nftables`, добавляя правила для разрешения или блокировки трафика.

107. Что такое трансляция сетевых адресов? Типы трансляции? Какие проблемы возникают при трансляции адресов?

Трансляция сетевых адресов (NAT) позволяет скрыть внутренние IP-адреса за одним публичным адресом. Основные типы: статическая, динамическая и PAT. Проблемы: сложности с сетевым мониторингом и несовместимость с некоторыми протоколами.

108. Как настроить трансляцию адресов в маршрутизаторах Mikrotik.

Используйте Winbox, создавая правило в разделе IP > Firewall > NAT.

109. Как настроить трансляцию адресов в операционной системе AstraLinux?

Используйте `iptables`, добавляя правила для NAT.

110. Модель OSI/ISO. Канальный и сетевой уровни: отличия и пример использования.

Модель OSI делит сетевые функции на 7 уровней. Канальный уровень отвечает за передачу данных между непосредственно связанными устройствами, тогда как сетевой уровень управляет маршрутизацией данных между различными сетями. Например, Ethernet работает на канальном уровне, а IP — на сетевом.

111. Как работают сетевой коммутатор, сетевой концентратор, сетевой мост?

Сетевой концентратор (хаб) принимает данные от одного устройства и отправляет их всем другим устройствам в сети. Он не фильтрует или обрабатывает данные, используемый в простых локальных сетях (LAN).

Сетевой мост (бридж) соединяет две или более сетевые сегменты, фильтруя трафик и снижая количество коллизий, передавая информацию только на те порты, где находятся целевые устройства.

Сетевой коммутатор (свитч) динамически управляет данными, отправляя их только конкретным устройствам на основе адресов MAC. Это повышает эффективность передачи данных и производительность сети.

112. Зачем используются сетевые мосты в маршрутизаторах?

Сетевые мосты помогают соединять разные сегменты сети, они могут работать в режиме "моста" для повышения производительности и управления трафиком.

Применяется на практике для разделения сетей по разным стандартам (например, PoE, Wi-Fi). Пример: в крупной организации, где сетевой организуется через разные этажи, мосты помогают соединить несколько локальных сетей в единую и управляемую.

113. Как настроить сетевой мост в маршрутизаторе Mikrotik? В AstraLinux?

Чтобы настроить мост в MikroTik:

Зайти в интерфейс WinBox или WebFig.

Перейти в раздел "Bridge".

Создать новый мост, добавив интерфейсы, которые необходимо объединить.

В AstraLinux это можно сделать через командную строку с помощью утилиты **bridge**, например:

```
ip link add name br0 type bridge  
ip link set dev eth0 master br0  
ip link set dev eth1 master br0
```

```
ip link set br0 up
```

114. Что такое цифровой шторм? Как от него защититься?

Цифровой шторм — это перегрузка сетевого трафика, вызванная внезапным увеличением запросов, что может привести к отказу в обслуживании (DoS). Защита включает настройку лимитов на трафик, использование систем обнаружения вторжений (IDS) и управление трафиком через брандмауэр.

115. Протокол определения колец STP. Зачем используется?

STP (Spanning Tree Protocol) предотвращает петли в сетях с избыточными соединениями. Он работает по принципу определения определенного "корневого" коммутатора и блокирует порты, создающие петли. Основные версии:

802.1D (стандартный)
Rapid STP (RSTP, 802.1w)
Multiple STP (MSTP, 802.1s)

116. Всегда ли обязательно использовать STP?

Не всегда. Плюсы включают защиту от петель, а минусы — задержки при переключении и сложность управления. Некоторые варианты сети могут обходиться без STP, если структуры сети не имеют избыточности.

117. Виртуальные локальные сети (VLAN): стандарт, зачем используются?

VLAN позволяют сегментировать сеть, создавая логические подгруппы в пределах одной физической сети. Это улучшает безопасность и управление трафиком. Например, в школе разные классы могут быть в отдельных VLAN для поиска данных. Максимальное количество VLAN в сети — 4096.

118. Могут ли быть одинаковые идентификаторы VLAN для разных портов маршрутизаторов?

Да, идентификаторы VLAN могут повторяться на разных устройствах, но это будут разные локальные сети. На одном коммутаторе или маршрутизаторе идентификаторы должны быть уникальными.

119. Как настроить в маршрутизаторе Mikrotik виртуальные интерфейсы для обработки тегированных пакетов?

Зайти в WinBox.
Перейти в "Interfaces".
Создать новый интерфейс типа "VLAN".

Указать нужный ID VLAN и интерфейс.

120. Как настроить в AstraLinux виртуальные интерфейс для обработки тегированных пакетов?

Пример настройки через командную строку:

```
ip link add link eth0 name eth0.10 type vlan id 10
```

```
ip link set dev eth0.10 up
```

Это создаст виртуальный интерфейс для обработки трафика VLAN с ID 10.